WHAT IS CLAIMED IS:

1. A computer network security system having enforceable security policy provision comprising:

means for providing variable security policy rule data for distribution to at least one network node;

means, operatively coupled to the means for providing, for associating a digital signature of a central security policy rule data distribution source to the variable security policy rule data;

means for storing the digital signature and the variable policy rule data; and

network node means, operatively coupled to the storage means, for obtaining the digital signature and the variable policy rule data and for analyzing the variable policy rule data to facilitate unilateral security policy enforcement at a network node level.

2. The computer network system of claim 1 wherein the means for providing includes user interface means for facilitating selection of variable security policy rule data.

3. The computer network system of claim 1 wherein the means for providing provides the variable security policy rule data from a data file.

4. The computer network system of claim 1 wherein the means for providing variable security policy rule data facilitates selection of variable security policy rule data on a per network node basis for central policy definition for the at least one network node.

5. The computer network system of claim 1 wherein the means for associating a digital signature of a central security policy rule data distribution source includes means

for associating a digital signature to the variable policy rule data to create a policy certificate.

6. The computer network system of claim 1 wherein the network node means includes:

means for storing variable policy rule data; and

means, operatively coupled to the means for storing , for using policy rule analysis data to decode the variable policy rule data to facilitate security policy enforcement at a network node level.

7. The computer network system of claim 1 wherein the variable policy rule data includes at least security policy identification data and policy rule setting data.

8. The computer network system of claim 7 wherein the variable policy rule data includes policy rule prioritization data.

9. The computer network system of claim 1 wherein the variable policy rule data includes differing policy rule data for a plurality of software applications supported by at least one network node and wherein the at least one network node includes means for facilitating cryptographic processing of data that is accessible by the plurality of software applications.

10. The computer network system of claim 1 wherein the means for storing the digital signature and the variable policy rule data stores a policy certificate for distribution to the network node under control of the network node.

11. The computer network system of claim 1 wherein the means for storing the digital signature and the variable policy rule data stores a policy certificate for distribution to the network nodes under control of the means for associating.

12. A computer network security system having enforceable security policy provision comprising:

means for storing variable security policy rule data for use by a network node; and

means, operatively coupled to the means for storing, for securely providing the variable security policy rule data for distribution to at least one network node to facilitate unilateral security policy enforcement at a network node level.

13. . The computer network system of claim 12 including user interface means for facilitating selection of variable security policy rule data for storage in the storage means.

14. The computer network system of claim 12 wherein the means for providing provides the variable security policy rule data from a data file.

15. The computer network system of claim 12 wherein the means for providing variable security policy rule data facilitates selection of variable security policy rule data on a per network node basis for central policy definition for the at least one network node.

16. A method for providing enforceable security policy provisions comprising:

providing variable security policy rule data for distribution to at least one network node;

associating a digital signature of a central security policy rule data distribution source to the variable security policy rule data;

storing the digital signature and the variable policy rule data; and

obtaining the digital signature and the variable policy rule data and analyzing the variable policy rule data to facilitate unilateral security policy enforcement.

17. The method of claim 16 wherein the step of providing variable security policy rule data includes facilitating selection of variable security policy rule data.

18. The method of claim 16 wherein providing variable security policy rule data includes facilitating selection of variable security policy rule data on a per network node basis for policy definition for at least one network node.

19. The method of claim 16 wherein associating a digital signature of a central security policy rule data distribution source includes associating a digital signature to the variable policy rule data to create a policy certificate.

20. The method of claim 16 wherein the step of obtaining the digital signature and the variable policy rule data includes:

storing variable policy rule data;

storing policy rule analysis data for evaluating the policy rule data; and

using the policy rule analysis data to decode the variable policy rule data to facilitate unilateral security policy enforcement at a network node level.

21. The method of claim 16 wherein the variable policy rule data includes at least security policy identification data, policy rule setting data and policy rule prioritization data.

22. The method of claim 16 wherein the variable policy rule data includes differing policy rule data for a plurality of software applications supported by at least one network node and wherein the at least one network node includes means for facilitating cryptographic processing of data that is accessible by the plurality of software applications.

23. The method of claim 16 wherein storing the digital signature and the variable policy rule data includes storing a policy certificate for distribution to the network nodes under control of the network nodes.

24. The method of claim 16 wherein storing the digital signature and the variable policy rule data includes storing a policy certificate for distribution to the network nodes under control of a network server.

25. A method for providing enforceable security policy provision comprising:

storing variable policy rule data for use by a network node; and

securely providing the variable security policy rule data for distribution to at least one network node to facilitate unilateral security policy enforcement at a network node level.

26. The method of claim 25 including facilitating selection of variable security policy rule data through a user interface.

27. The method of claim 25 wherein securely providing includes providing the variable security policy rule data from a data file.

28. The method of claim 25 wherein providing variable security policy rule data includes facilitating selection of variable security policy rule data on a per network node basis for central policy definition for the at least one network node.

29. A computer having enforceable security policy provision comprising:

means for obtaining variable policy rule data from a central security policy rule data distribution source;

means, operatively coupled to the means for obtaining, for analyzing the variable policy rule data; and

means, responsive to the means for analyzing the variable policy rule data, for facilitating unilateral security policy enforcement at a network node level based on the variable policy rule data.

30. The computer of claim 29 wherein the means for obtaining includes means for storing variable policy rule data, and wherein the means for analyzing the variable policy rule data includes means for storing policy rule analysis data for evaluating the policy rule data and means, operatively coupled to the means for storing and the means for storing policy rule analysis data, for using the policy rule analysis data to decode the variable policy rule data to facilitate security policy enforcement at a network node level.

31. The computer of claim 29 wherein the variable policy rule data includes differing policy rule data for a plurality of software applications supported by the computer and wherein the computer includes means for facilitating cryptographic processing of data that is accessible by the plurality of software applications.

32. The computer of claim 29 wherein the variable policy rule data includes at least security policy identification data and policy rule setting data.

33. The computer of claim 29 wherein the variable policy rule data includes policy rule prioritization data and wherein the means for periodically obtaining obtains a digital signature corresponding to the policy rule data.

34. A storage medium for storing programming instructions that, when read by a processing unit, causes the processing unit to provide enforceable security policy provision, the storage medium comprising:

first means for storing programming instructions that facilitate storing variable security policy rule data for use by a network node; and

second means for storing programming instructions that facilitate providing the variable security policy rule data for distribution to at least one network node to facilitate unilateral security policy enforcement at a network node level.

35. The storage medium of claim 34 wherein the first means for storing programming instructions stores programming instructions that, when read by a processing unit, causes the processing unit to facilitate selection of variable security policy rule data.

36. The storage medium of claim 34 wherein the first means for storing programming instructions stores programming instructions that, when read by a processing unit, causes the processing unit to facilitate selection of variable security policy rule data on a per network node basis for policy definition for to at least one network node.

37. The storage medium of claim 34 wherein the first means for storing programming instructions stores programming instructions that, when read by a processing unit, causes the processing unit to associate a digital signature of a central security policy rule data distribution source by associating a digital signature to a policy rule data to create a policy certificate.

38. The storage medium of claim 37 wherein the first means for storing programming instructions stores programming instructions that, when read by a processing unit, causes the processing unit to store the variable policy rule data that includes at least security policy identification data and policy rule setting data.